IBM HTTP Server and SSL Certificates

> Refer to Apache and SSL Certificates for conceptual references.

Once installed, IHS includes a tool for working with SSL Certificates called **IBM's Key Management Utility** which IBM also refers to as GSKIT and generally referred to as **iKeyMan**. We will use iKeyman consistently in this documentation.

> Something that I have not tried yet but should work in theory. To make things easier, use the open ssl command line tools to generate the CSR. When the CA gives back the signed request, generate a P12. Make sure to also include the private key somehow. Then you should be able to import into IHS and delete the old certificate.

Verify Version

Most current installs should be fine. However, you should still ensure that the iKeyMan packaged with IHS can start and is the minimal version for 2048 certificates. 2048 is now becoming the minimal standard for Web certificates.

To start iKeyman regardless of the environment you must specify a JAVAHOME which points to a version of Java with JCE. IBM should have packaged the right version of java for you. On Windows, use the icon from the start menu which does this for you.

> I actually don't remember why I have these instructions actually.

... not sure if needed START ...

Go the command line and issue the following commands,

```
E:\
cd opt\IBMIHS\gsk7\bin
set JAVA_HOME=E:\opt\IBMIHS\java\jre
gsk7ikm.exe
```

... not sure if needed END ...

Which should launch iKeyman. Click Help and then About iKeyman and confirm the version to be higher than 7.0.3.18.

Create Key Database File

IBM uses the concept of a Key Database File to protect the certificate private key. The first step is to create an empty key database file using iKeyMan.

1. Key Database File
2. New
3. Key database type = CMS (can explain more about the format... later but CMS if standard)
4. File Name = krypton.kdb

5. Browser... = C:\opt\IBMIHS\keys\

You will the **Password Prompt** window appears check **Stash password to a file**. Enter in a password which will from now on be used to protect the key database file and click OK.

> Stashing the password will keep the password with IHS. This means that IHS will be able to be stopped and started without requiring you to enter in the password to the key database file every time.

Generate CSR for Web Server

Confirm your key database file is loaded. The iKeyman window should now show,

DB-Type: CMS
File Name: C:\opt\IBMIHS\keys\krypton.kdb

Next generate the CSR as follows,

1. In the middle of the iKeyman Window locate a section called **Key database content**.
2. Change the Key database content drop down from the default, Signer Certificates to Personal Certificate Requests.
3. Create
4. New Certificate Request...

At the Create New Key and Certificate Request window fill in the details. Here is an example,

> **Key Label = www.krypton.com-2012-03-13**
> **Key Size = 2048**
> Signature Algorithm = SHA1WithRSA
> **Common Name = www.krypton.com**
> Organization = Acme
> Organizational Unit = Publishing
> Locality = Toronto
> State/Province = ON
> Zipcode =
> Country or region = CA

Key Label is the name that shows up in the key store file and is arbitrary. It is recommended to use the domain name since it is unique combined with the date the CSR is created. this is because most CAs do not support certificate renewals. During the certificate renewal exercise you will need to create a new CSR while maintaining the original key store.

Key Size is set to 2048. Most modern CAs will not accept less than 2048.

Common Name though it is marked as optional is technically not. It must be the domain name of your website.

Note the location and file name of the certificate request. Change the default name, or you may end up overwriting previous other certificate requests. In this example it would be **C:\opt\IBMIHS\keys\www.krypton.com.2012-03-13.certificate_request.arm**.

Click OK.

Upon success you will see the following message,

> A new certificate reqweuest has been successfully created in the file: C:\opt\IBMIHS\keys\www.krypton.com.2012-03-13.certificate_request.arm. Send the file to a certification authority to request a certificate.

There will now be a certificate request as an item in the **Key database content** section.

> Do not use click the save button. It actually makes things confusing as it really is a save as... button.

Exit iKeyman which will also auto-save your changes.

Verify CSR

...

Backup Private Key

Backup all key related files. In this example, C:\opt\IBMIHS\keys\krypton.* should be copied.

Submit CSR

Send the **arm** file to your Certificate Authority.

Import Private Key

The Certificate Authority will provide a signed certificate file, root certificate and possibly supporting chain certificates which will be imported into your kdb file.

Backup Your Files (Again!)

iKeyMan saves to the Key Database File arbitrary depending on your action and saves things across **multiple** files. Backup your files before proceeding.

> Remember **backup** the **complete set** together. In this example that would be all files **krypton.*** and not just krypton.kdb.

If your files become corrupt, the entire process will need to be restarted.

Rename CA Provided Certificates

In addition to the signed certificate, the CA should include the Root Certificate and any required supporting Chain Certificates. It is important to use a consistent naming convention.

...

The signed certificate will often be in a plain txt file. Rename the file to C:\opt\IBMIHS\keys\www.krypton.com.2012-03-14.signed_certificate.arm

The date included in the file name should reference when the certificates were received.

Import Root Certificate

...

Import Signed Certificate

If necessary, start iKeyMan and open the key database.

- From the Windows desktop, select Start - Programs - IBM HTTP Server - Start Key Management Utility.
- Select Key Database File - Open and open the "Httpserverkey.kdb" database in the C:\Program Files\IBM\WebSphere\AppServer\etc directory.

In the "Key database content" drop-down list, select "Personal Certificates."

On the right-hand side of the "Key database content" box, click the "Receive..." button.

In the "Receive Certificate from a file" window, complete the following fields:

- Data type: Accept the default of "Base64-encoded ASCII data."
- Certificate file name: Browse to and select the "HTTPServerCert.cer" file (or other server certificate file that you have obtained from the CA).
- Location: Ensure the location field specifies the directory path to which the "HTTPServerCert.cer" file was saved after you received the file from the CA (for example C:\Program Files\IBM\WebSphere\AppServer\etc).

Click OK.

You should now see the server certificate name displayed in the Personal Certificates list in IKeyMan.

> The server certificate name was selected when creating the CSR.

References

Has good steps and pictures - http://www-01.ibm.com/support/docview.wss?uid=swg21006430

Steps to Importing Signed Certificate with iKeyMan - http://publib.boulder.ibm.com/infocenter/sametime/v8r0/index.jsp?topic=/com.ibm.help.sametime.801.doc/EMS/st_adm_ems_ssl_cert_for_http_t.html